# DEV270
# Windows XP Service Pack 2
## *Information for Developers*

**Tony Goodhew**
**Product manager**
**Developer Division**
**Microsoft Corp**
**tgoodhew@microsoft.com**

Microsoft Tech·Ed 2004

# Agenda

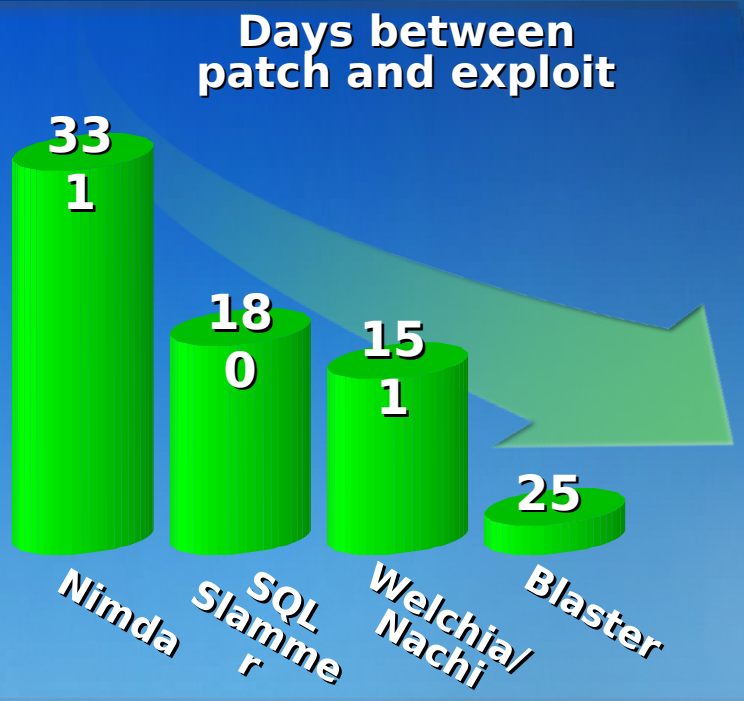
- Windows® XP Service Pack 2 Overview
- Developer Calls-To-Action

Microsoft Tech·Ed 2004

# Background

## Responding to the Crisis

- Exploits proliferating
- Time to exploit decreasing
- Exploits are more sophisticated
- Current approach is insufficient




**Security is a top priority**
**No silver bullet: the solution is complex**
**Change requires innovation**

Microsoft Tech·Ed 2004

# Securing Today's World

- Windows XP SP2
  - Firewall on by default
  - All outstanding fixes (QFE, Security, Customer)
  - Safer email and Web browsing
  - Enhanced memory protection


Available to developers at:

http://msdn.microsoft.com/security

http://www.microsoft.com/windowsxp

# Windows XP SP2 Overview

| | |
|---|---|
| Network | Help protect the system from directed attacks from the network |
| Email/IM | Helps provide security for Email and Instant Messaging experience |
| Web | Helps provide security for Internet experience for most common Internet tasks |
| Memory | Offer system-level protection for the base operating system |

Microsoft Tech·Ed 2004

# Windows firewall

**Network**

Email/IM

Web

Memory

## Intended Goal and Customer Benefit

- Offer increased protection from network attacks by default
- Focused on roaming systems, small business, home users

## What We're Doing

- Windows Firewall (formerly ICF) will be on by default
- More configuration options
  - Group policy, command line, unattended setup
  - Enhanced user interface
- Boot time protection
- Multiple profile support
  - Connected to corporate network vs. home
- Enable file sharing on home networks with Windows Firewall

## Developer Call-to-Action

- In-bound network connections, by default, are not permitted
- Dynamically enable ports as necessary, but only for as long as necessary, disable when done

Microsoft Tech·Ed 2004

# Demo

## Windows Firewall

Microsoft Tech·Ed 2004

# DCOM and RPC changes

**Network**

Email/IM

Web

Memory

Intended Goal and Customer Benefit

- Reducing DCOM / RPC attack surface exposed on network

What We're Doing

- Require authentication on default interfaces
- Offer programmatic ability to restrict RPC interfaces to local machine only
- Configuration of access and launch permissions for DCOM through registry
- Move most RPCSS code into reduced privilege process
- Offer customer-controlled option to require authentication to the end-point mapper
- Disable RPC over UDP by default

Developer Call-to-Action

- Where appropriate, use new RPC API to limit calls to local machine
- Ensure your application doesn't require anonymous clients
- Don't use RPC over UDP

Microsoft Tech·Ed 2004

# Demo

## DCOM Security

Microsoft Tech·Ed 2004

# Email Attachments

Network

**Email/IM**

Web

Memory

Intended Goal and Customer Benefit

- System-provided mechanism for applications, intended to provide security for unsafe attachments
- Consistent user experience for attachment “trust” decisions

What We’re Doing

- Offering new public API for handling of attachments (Attachment Execution Services)
- Default to “not trust” unsafe attachments
- Outlook®, Outlook® Express, Windows® Messenger, Internet Explorer updated to make use of new API
- Security enhanced message “preview”
- Replaces **`AssocIsSafe()`**

Developer Call-to-Action

- Use new API in your applications for better user experience, and better identification of potentially unsafe content

Microsoft Tech·Ed 2004

# Demo

## Attachment Execution Services

Microsoft Tech·Ed 2004

# Web Browsing

Network

Email/IM

**Web**

Memory

Intended Goal and Customer Benefit

- Offer a security enhanced web browsing experience

What We're Doing

- Locking down local machine and local intranet zones
- Improving notifications for running or installing applications and ActiveX® controls
- HTML files on the local machine will not be able to script potentially unsafe ActiveX controls or access data across domains in the Local Machine Security Zone
- Blocking unknown, unsigned ActiveX controls
- Disarm cross domain script attacks on APIs
- Improved detection and handling of downloaded files through improvements to mime-handling code path
- Files served with mismatched or missing mime-headers and file extensions may be blocked

Microsoft Tech·Ed 2004

# Web Browsing (cont'd)

Network

Email/IM

**Web**

Memory

What We're Doing (continued)

- Mitigate ActiveX® reuse through potential limited control leashing and increased amount of guided user experience
- Limit UI spoofing
- Pop-up windows will be suppressed unless they are initiated as a result of user action

Developer Call-to-Action

- Check for web application compatibility with newly enhanced browsing defaults
- Identify whether controls are safe for scripting on the Internet, or if they can be more restricted

Microsoft Tech·Ed 2004

# Demo

## IE Changes

Microsoft Tech·Ed 2004

# Data Execution Protection

Network

Email/IM

Web

**Memory**

Intended Goal and Customer Benefit

- Reduce exposure of some buffer overruns

What We're Doing

- Leverage hardware support in 64-bit and newer 32-bit processors to only permit execution of code in memory regions specifically marked as execute
- Reduces exploitability of buffer overruns
- Enable by default on all capable machines for Windows binaries

Developer Call-to-Action

- Ensure your code doesn't execute code in a data segment
- Ensure your code runs in PAE mode with <4GB RAM
- Use VirtualAlloc with PAGE_EXECUTE to allocated memory as executable
- Test your code on 64-bit and 32-bit processors with "Execution protection"

Microsoft Tech·Ed 2004

# Demo

## Data Execution Prevention

Microsoft Tech·Ed 2004

# SP2 Call-To-Action

- Right now
  - Write secure code!
    - Read Writing Secure Code, Second Edition by Michael Howard (MSPress)
  - Ensure your applications work with a host firewall enabled
  - Get the Service Pack from MSDN and test your applications
- Immediate Future
  - Test your code with non-executable memory on 64-bit or capable 32-bit processors
- For more information, see
  - http://msdn.microsoft.com/security

Microsoft Tech·Ed 2004

Microsoft®

© 2003-2004 Microsoft Corporation. All rights reserved. Windows, Microsoft, Outlook and ActiveX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Microsoft Tech·Ed 2004